The serialization title

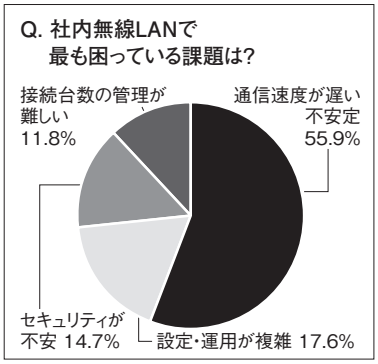
情報システム担当が選ぶネットワークインフラ

第3回 社内「Wi-Fi」を刷新するときが来た

株式会社ピーエスアイ
管理部広報担当
内藤 純一
URL https://www.psi.co.jp
E-mail support@psi.co.jp

Web会議中のフリーズ、電波が届かない座席など、弊社がX（旧Twitter）で実施したアンケート（図1）によると、55.9%が「通信速度が遅い・不安定」を最大の課題に挙げており、その背景には業務に適さない家庭用機器の流用、設計なきAP（アクセスポイント）増設があります。本稿で、不安定の根本原因を明らかにし、エンタープライズ無線LANへの移行による、速度・セキュリティ双方の向上について実践的に解説します。

図1　アンケート結果（回答数68票）



Wi-Fi通信が不安定な本当の原因

●Wi-Fiの通信速度が遅い…

この苦情を受けた際に、担当者が最初に行う対策が「AP（アクセスポイント）を増やすこと」です。多くのケースで、量販店で数千円から数万円のルーターを購入し、電波が弱いとされるエリアに追加設置します。

一見、理にかなった対策のように思えますが、実は、これが状況をさらに悪化させる最大の要因となっている場合が多く、無計画なAP増設は深刻な「電波干渉」を引き起こし、通信品質を著しく低下させます。

Wi-Fi通信において、特に広く利用されている2.4GHz帯は、利用できる周波数帯域（チャネル）が非常に限られています。

お互いが干渉することなく同時に通信できるチャネルは、実質的には「1」「6」「11」の3つしかありません。近隣のオフィスから漏れてくる電波に加え、自社内で無計画に設置したAP同士が同じチャネルを取り合うことで、電波の空中衝突が発生します。

Wi-Fiは「誰かが話している間は、他の人は黙って待つ」といった仕組みのCSMA／CA方式を採用しているため、干渉が増えれば増えるほど、通信待ちの時間（レイテンシ）が増大し、実効速度が低下します。

●隠れ端末問題

これも日本のオフィス環境特有の課題です。パーテーションや壁で仕切られると、端末Aと端末Bがお互いの電波を検知できない位置関係になることがあります。

この状態で両者が同時にAPへデータを送信すると、AP側でデータが衝突（コリジョン）して通信エラーとなり、再送処理が頻発することからネットワーク全体の

図２　家庭用ルーターと業務用 AP の違い

■ 家庭用ルーター	■ 業務用ＡＰ
・**想定接続台数**：5 ～ 10 台程度（家族利用を想定）	・**想定接続台数**：30 ～ 100 台以上（高密度環境に対応）
・**アンテナ**：全方向に均等に電波を飛ばします（無指向性）	・**アンテナ**：端末の位置を狙って電波を届けます（ビームフォーミング）
・**ローミング**：端末任せ（移動すると切れることが多い）	・**ローミング**：ＡＰ側が主導してスムーズに切り替えます
・**設計思想**：動画視聴など下り通信中心の「ベストエフォート」	・**設計思想**：多数同時接続時の公平性（エアタイムフェアネス）

パフォーマンスが劇的に低下する現象です。ＡＰを増やせば増やすほど、この「隠れ端末問題」が発生する確率は高まっていきます。

加えて、オフィス内にはＷｉ‐Ｆｉ以外の干渉源も多数存在します。電子レンジ、Bluetooth 機器、コードレス電話などは、Ｗｉ‐Ｆｉと同じ2.4ＧＨｚ帯を使用するため、これらが稼働するたびに通信が断続的に途切れる原因となります。よくランチタイムに「つながりにくい」という現象が起きるのは、電子レンジの使用と無関係ではありません。

●廉価な機器を使用している

しかし、根本的な原因の多くは中小企業が「家庭用ルーター」や廉価な「ＳＯＨＯ向け機器」を、そのままオフィスの基幹インフラとして使用していることにあります。家庭用ルーターと業務用（エンタープライズ）ＡＰは、外見こそ似てはいるものの、その設計思想は全く異なります（図2）。

家庭用ルーターは、家族数人が動画を見たりネットサーフィンをしたりすることを想定して設計されており、ＣＰＵ性能やメモリ容量もそれに見合ったものです。

一方、現代のオフィスでは、一人の従業員が複数のデバイス（ＰＣとスマートフォン、タブレットなど）を接続することも珍しくありません。30人の従業員がいれば接続デバイス数は容易に50台を超えます。この規模の接続を家庭用ルーター1台で処理しようとすれば、処理能力の限界を超えてしまい、フリーズや再起動を繰り返すのは当然の結果といえます。

「Ｗｉ‐Ｆｉ６」の革新的な3つのポイント

こうした「混雑さ」「不安定さ」を技術的に解決するために登場したのが、最新規格の「Ｗｉ‐Ｆｉ６（IEEE802.11ax）」です。これは単に最高速度を向上させるだけではなく、多数のデバイスが同時接続しても遅くならないことを主眼に開発された規格です。

「High Efficiency Wireless（高効率無線）」とも呼ばれる革新性は次の3つの技術に集約されます。

①ＯＦＤＭＡ（直交周波数分割多元接続）技術

従来のＷｉ‐Ｆｉ（Ｗｉ‐Ｆｉ５以前）は、荷物（データ）を運ぶ際、トラック（通信フレーム）の荷台が空いていても必ず1台で配送するような非効率な通信を行っていました。つまり、小さなデータを送るだけでも帯域全体を占有してしまい、順番待ちが発生していたのです。

Ｗｉ‐Ｆｉ６のＯＦＤＭＡは、1台のトラックに複数の宛先の荷物を「相乗り」させる技術です。

1回の通信フレームを細かく分割し、最大74ユーザー分のデータを同時に運ぶことができます。

これにより、多数のデバイスが同時に通信しても待ち時間（レイテンシ）が劇的に減少し、Ｗｅｂ会議の遅延などが解消されます。

②ＭＵ‐ＭＩＭＯ（マルチユーザー・マイモ）の進化

これは、ＡＰが複数のアンテナを使って、複数の端末と同時にデータの送受信を行う技術です。

Ｗｉ‐Ｆｉ５でも、ダウンロード方向のみ対応していましたが、Ｗｉ‐Ｆｉ６ではアップロード方向にも対応しました。

従来のＷｉ‐Ｆｉが「１対１」の通信を高速に切り替えていたのに対して、Ｗｉ‐Ｆｉ６は真の意味での「同時通信」を実現しています。これにより、大容量データのアップロードやクラウドストレージへのバックアップ時でも、他のユーザーの通信を阻害しにくくなりました。

③ BSS Coloring による干渉制御

BSS Coloringは、特にＡＰが密集するオフィスビル環境で威力を発揮します。自ネットワークの通信パケットに「色（Color）」という識別子を付けることで、隣接するＡＰからの電波（異なる色）を検知しても、それが一定の干渉レベル以下であれば「無視」して通信を継続する技術です。

従来は、隣りの微弱な電波を検知しただけで通信を待機していましたが、BSS Coloringにより、物理的に混雑した環境でもスループット（実効速度）が低下しにくくなっています。

さらに、２０２２年９月に日本国内でも解禁された「Ｗｉ‐Ｆｉ６Ｅ」登場の影響も大きく、これは、Ｗｉ‐Ｆｉ６の機能をそのままに、新たに「６ＧＨｚ帯」を利用可能にしたものです。

2.4ＧＨｚ帯や５ＧＨｚ帯は、電子レンジや気象レーダー、近隣のＷｉ‐Ｆｉなど多くの電波で溢れかえっています。対して６ＧＨｚ帯は、現時点ではＷｉ‐Ｆｉ専用の広大な帯域であり、いわば「渋滞知らずの専用道路」です。チャネル数も豊富で、干渉を気にせず広帯域（１６０ＭＨｚ幅など）を利用できるため、圧倒的な高速通信と低遅延を実現します。

これらの技術革新により、Ｗｉ‐Ｆｉ６／６Ｅ環境では、30人が一斉にＷｅｂ会議に参加しても映像が固まらず、ＳａａＳ※型業務アプリケーションのレスポンスも有線ＬＡＮ並みに安定します。

「速いだけではなく混雑に強い」という特性こそが、エンタープライズ環境においてＷｉ‐Ｆｉ６が必須とされる所以です。

※ SaaS：インターネット経由でソフトウェアをクラウドサービスとして利用できる仕組み。

無線ＬＡＮ特有の脅威とは

無線ＬＡＮには、有線ＬＡＮにはない特有のリスクがあり、それは「電波が建物の外まで漏れ出る」という物理的な特性です。攻撃者はオフィスの外の駐車場や隣のビルから、社内ネットワークへの侵入を試みることができます。

アンケートでも約15％が「セキュリティが不安」と回答していますが、実際の脅威はその不安以上に深刻です。ここでは、無線ＬＡＮ特有の３つの主要な脅威と対策について解説します。

①不正ＡＰ（Evil Twin：悪魔の双子）の脅威

これは、悪意ある攻撃者が正規の社内Ｗｉ‐Ｆｉと同じＳＳＩＤ（ネットワーク名）を設定した「偽ＡＰ」を設置する手口です。

ＰＣやスマートフォンは、過去に接続したことのあるＳＳＩＤを見つけると自動的に接続する性質があります。従業員の端末が誤ってこの偽ＡＰに接続してしまうと、通信内容をすべて盗聴されるだけではなく、偽のログイン画面へ誘導されてＩＤやパスワードを搾取される恐れがあります。

これを防ぐには、社内ネットワーク内に許可されていないＡＰが存在しないかを常時監視し、検知・遮断するＷＩＰＳ（無線侵入防止システム）の導入が有効です。

②パスワードの共有運用

多くの中小企業では、家庭用と同様の「WPA2-Personal（PSK）」方式を採用し、全社員が同じパスワード（事前共有鍵）を使い回しています。この運用では、退職者が出るたびに全端末のパスワードを変更しなければならず、実務上ＮＧと断言できます。

つまり、退職者がオフィスの近くから社内Ｗｉ‐Ｆｉに接続できてしまう、あるいはパスワードを知る部外者が容易に侵入できるというセキュリティホールが放置されることになります。

それを解決するのが「WPA2/

WPA3-Enterprise（802.1X認証）」であり、これは全員共通のパスワードではなく、ユーザーごとのID・パスワード（PEAP認証）や、デバイスごとの「電子証明書」（EAP-TLS認証）を用いて認証を行う方式です。

特にEAP-TLSは、会社が発行した証明書を持つ端末しか接続できないため、セキュリティ強度が極めて高く、パスワード漏えいのリスクがないうえに、従業員が許可なく持ち込んだ私物スマートフォン（シャドーIT）の接続も物理的に防ぐことができます。

退職時には、その端末の証明書を失効させるだけでよく、運用負荷も低くてすみます。

③最新のセキュリティ規格「WPA3」への移行も重要

WPA3では、新しい鍵交換方式「SAE（Simultaneous Authentication of Equals）」が採用され、従来のWPA2で脆弱とされていた「辞書攻撃」や「オフライン総当たり攻撃」への耐性が飛躍的に向上しています。仮に、単純なパスワードを設定していたとしても、外部から解析されるリスクが大幅に低減されるようになりました。

正しいAP設計の要点

●電波調査とカバレッジ

高価なエンタープライズAPを購入しても、その配置や設定が不適切であれば、本来の性能を発揮することはできません。正しい無線LAN環境を構築するためには、事前の設計（プランニング）が何よりも重要です。

設計の第一歩は「サイトサーベイ（電波調査）」です。

オフィスの図面上だけでAPの台数を計算するのではなく、実際に現場で壁の材質や厚さ、スチール棚の配置などを確認して電波の飛びをチェックします。

これは、専用の測定器がなくても、スマートフォンの無料アプリ（Wi-Fi Analyzerなど）を使えば簡易的な測定は可能です。電波が届かないデッドスポットがないか、隣接するオフィスの強力な電波と干渉していないかを確認し、最適な設置場所を選定します。

APの配置において重要な原則は「カバレッジ」の重複です。

隣接するAP同士の通信範囲（セル）が、互いに15～20％程度重なるように配置するのが理想的とされます。この重複エリアによって、ユーザーが端末を持って歩きながら移動した際、接続先のAPがスムーズに切り替わる（ローミング）ことができます。

重複が少なすぎると接続が切れる原因となり、逆に多すぎると干渉の原因となるため、APの送信出力を調整して適切なオーバーラップを維持することが肝要です。

●管理方式の選択

中小企業は、インターネット経由で一元管理できる「クラウド管理型」のAPが主流であり、現地にコントローラサーバーを設置する必要がないため導入コストを抑えられるほか、ファームウェアの自動更新やリモートからの設定変更も可能になります。

情シス担当者が不在の拠点や在宅勤務中のトラブルシューティングにおいても、クラウド管理画面から状況を把握できるメリットは計り知れません。

【まとめ】

昨今、無線LANは「あれば便利」な設備ではなく、業務継続に不可欠な「ライフライン」です。

家庭用機器による場当たり的な運用は、業務効率の低下を招くだけではなく、情報漏えいなどのセキュリティ事故に直結するリスクを孕んでいます。

Wi-Fi6／6E対応のエンタープライズAPへの投資は、快適な業務環境と堅牢なセキュリティを同時に手に入れることができ、中長期的に見れば極めて費用対効果の高い施策です。問題が起きてから対処するのではなく、正しい知識と設計に基づいたインフラ刷新を行うことが、企業の競争力を支える土台となります。